AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (previously presented): An AES encryption processor comprising:

a selector unit selecting an element of a state in response to row and column indices;

a substitution unit for obtaining a substitution value with said selected element used as an index;

a coefficient table providing first to fourth coefficients in response to said row index;

first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients, respectively, the first to fourth products corresponding to a same one column of the state; and

an accumulator which accumulates the first to fourth products corresponding to all four columns of the state to develop first to fourth elements of a designated column of a resultant state.

2. (original): The AES encryption processor according to claim 1, wherein said first to fourth coefficients are respectively set

to {02}, {01}, {01}, and {03} in response to said row index selecting a first row of said state,

to {03}, {02}, {01}, and {01} in response to said row index selecting a second row of said state,

to {01}, {03}, {02}, and {01} in response to said row index selecting a third row of said state, and

to {01}, {01}, {03}, and {02} in response to said row index selecting a fourth row of said state.

3. (previously presented): An AES encryption processor adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state, said AES encryption processor comprising:

a selector unit selecting an element of said state in response to said first operand and said immediate operand, said selected element being stored in said input register;

a S-box for obtaining a substitution value with said selected element used as an index;

a coefficient table providing first to fourth coefficients in response to said immediate operand;

first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively; and

a storing unit for storing said first to fourth products into said output register selected by said second operand.

4. (original): The AES encryption processor according to claim 3, further comprising a processing unit adapted to implement XORing,

wherein said AES encryption processor is further adapted to an XOR instruction, and

wherein said processing unit implements XORing of values contained in two selected registers of said register file.

5. (original): The AES encryption processor according to claim 1, wherein said first to fourth coefficients are respectively set

to {02}, {01}, {01}, and {03} in response to said row index selecting a first row of said state,

to {03}, {02}, {01}, and {01} in response to said row index selecting a second row of said state,

to {01}, {03}, {02},and {01} in response to said row index selecting a third row of said state, and

to {01}, {01}, {03}, and {02} in response to said row index selecting a fourth row of said state.

6. (previously presented): An AES decryption processor comprising:

a selector unit selecting an element of a state in response to row and column indices;

an inverse S-box for obtaining a substitution value with said selected element used as an index;

a coefficient table providing first to fourth coefficients in response to said row index;

first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively; and

an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state.

7. (previously presented): The AES decryption processor according to claim 6, wherein said first to fourth coefficients are respectively set

to {02}, {01}, {01}, and {03} in response to said row index selecting a first row of said state,

to {03}, {02}, {01}, and {01} in response to said row index selecting a second row of said state,

to {01}, {03}, {02}, and {01} in response to said row index selecting a third row of said state, and

to {01}, {01}, {03}, and {02} in response to said row index selecting a fourth row of said state.

8. (previously presented): An AES decryption processor adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state, said AES decryption processor comprising:

a selector unit selecting an element of said state in response to said first operand and said immediate operand, said selected element being stored in said input register;

a S-box for obtaining a substitution value with said selected element used as an index;

a coefficient table providing first to fourth coefficients in response to said immediate operand;

first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively; and

a storing unit for storing said first to fourth products into said output register selected by said second operand.

9. (previously presented): The AES decryption processor according to claim 8, further comprising a processing unit adapted to implement XORing,

wherein said AES decryption processor is further adapted to an XOR instruction, and

wherein said processing unit implements XORing of values contained in two selected registers of said register file.

10. (original): The AES encryption processor according to claim 8, wherein said first to fourth coefficients are respectively set

to {02}, {01}, {01}, and {03} in response to said row index selecting a first row of said state,

to {03}, {02}, {01}, and {01} in response to said row index selecting a second row of said state,

to {01}, {03}, {02}, and {01} in response to said row index selecting a third row of said state, and

to {01}, {01}, {03}, and {02} in response to said row index selecting a fourth row of said state.

11. (previously presented): An AES processor comprising:

a first selector unit selecting an element of a state in response to row and column indices;

an inverse affine transformation circuit applying an inverse affine transformation on said selected element;

a second selector unit selecting one out of two data bytes consisting of said selected element received from said first selector, and a result of said inverse affine transformation received said inverse affine transformation circuit, wherein said selected element is selected for encryption, while said result of said inverse affine transformation is selected for decryption;

an inverse determining unit obtaining a multiplicative inverse of said selected data byte received from said second selector;

an affine transformation circuit applying an affine transformation on said obtained multiplicative inverse;

a third selector unit selecting one of two data bytes consisting of said multiplicative inverse received from said inverse determining unit, and a result of said affine transformation received from affine transformation circuit, wherein said result of said affine transformation is selected for decryption, while said multiplicative inverse is selected for encryption;

a coefficient table providing first to fourth coefficients in response to said row index;

first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively; and

an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state.

12. (previously presented): An AES processor adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state, said AES processor comprising:

a first selector unit selecting an element of said state in response said first operand and said immediate operand, said selected element being stored in said input register;

an inverse affine transformation circuit applying an inverse affine transformation on said selected element;

a second selector unit selecting one out of two data bytes consisting of said selected element received from said first selector, and a result of said inverse affine transformation received said inverse affine transformation circuit, wherein said selected element is selected for encryption, while said result of said inverse affine transformation is selected for decryption;

an inverse determining unit obtaining a multiplicative inverse of said selected data byte received from said second selector; an affine transformation circuit applying an affine transformation on said obtained multiplicative inverse;

a third selector unit selecting one of two data bytes consisting of said multiplicative inverse received from said inverse determining unit, and a result of said affine transformation received from affine transformation circuit, wherein said result of said affine transformation is selected for decryption, while said multiplicative inverse is selected for encryption;

a coefficient table providing first to fourth coefficients in response to said row index;

first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively; and

a storing unit for storing said first to fourth products into said output register selected by said second operand.

13. (original): The AES processor according to claim 12, further comprising a processing unit adapted to implement XORing,

wherein said AES processor is further adapted to an XOR instruction, and

wherein said processing unit implements XORing of values contained in two selected registers of said register file.

14. (previously presented): An AES processor adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state(s), said AES processor comprising:

a plurality of AES processor cores respectively associated with a plurality of columns of said state(s); and

a coefficient table providing first to fourth coefficients in response to said immediate operand;

wherein each of said plurality of AES processor cores includes: a first selector unit selecting an element of said state(s) in response said first operand and said immediate operand, said selected element being stored in said input register, an inverse affine transformation circuit applying an inverse affine transformation on said selected element, a second selector unit selecting one out of two data bytes consisting of said selected element received from said first

selector, and a result of said inverse affine transformation received said inverse affine transformation circuit,

wherein said selected element is selected for encryption, while said result of said inverse affine transformation is selected for decryption, an inverse determining unit obtaining a multiplicative inverse of said selected data byte received from said second selector, an affine transformation circuit applying an affine transformation on said obtained multiplicative inverse, a third selector unit selecting one of two data bytes consisting of said multiplicative inverse received from said inverse determining unit, and a result of said affine transformation received from affine transformation circuit,

wherein said result of said affine transformation is selected for decryption, while said multiplicative inverse is selected for encryption, first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively, and a storing unit for storing said first to fourth products into said output register selected by said second operand.

15. (previously presented): The AES encryption processor according to claim 1, wherein the first to fourth multipliers are Galois field multiplexers.

16. (new): The AES encryption processor according to claim 1, wherein the selector unit also selects other elements of the state in response to the row and column indices, respectively, and the substitution unit also obtains other substitution values of each of the other selected elements of the state with each of the other selected elements used as an index, respectively.

17. (new): The AES encryption processor according to claim 16, wherein the first to fourth multipliers respectively, also compute other first to fourth products, which are obtained by multiplying said substitution values of the each of the other selected elements with the first to fourth coefficients, respectively, each of the other first to fourth products corresponding to different columns of the state.

18. (new): The AES encryption processor according to claim 17, wherein the all four columns comprises the different columns of the state and the same one column of the state.

19. (new): The AES encryption processor according to claim 1, wherein the accumulator adds each of the four columns of the state to develop first to fourth elements of the designated column of the resultant state.

20. (new): The AES encryption processor according to claim 1, wherein the substitution value is provided to the first to fourth multipliers.